

CLAIMS

What is claimed is:

1 1. A method for providing recipient-end security for transmitted data, the
2 method comprising:
3 scanning a hard copy document to generate scanned data;
4 configuring the scanned data so as to require recipient-end security;
5 transmitting the scanned data to an intended recipient;
6 determining if the transmitted data may be accessed at the recipient end; and
7 denying access to the transmitted data if it is determined that the transmitted
8 data may not be accessed.

1 2. The method of claim 1, wherein scanning a hard copy document
2 comprises scanning a hard copy document using a data transmitting device that
3 transmitted the scanned data to an intended recipient.

1 3. The method of claim 1, wherein configuring the scanned data
2 comprises configuring the scanned data such that recipient-specific security
3 information must be provided by a recipient of the transmitted data prior to accessing
4 the transmitted data.

1 4. The method of claim 3, wherein configuring the scanned data
2 comprises configuring the scanned data such that the recipient must provide at least
3 one of a recipient password and recipient biometric information to access the
4 transmitted data.

1 5. The method of claim 1, wherein configuring the scanned data
2 comprises configuring the scanned data such that machine-specific security data must
3 be verified prior to accessing the transmitted data.

1 6. The method of claim 5, wherein configuring the scanned data
2 comprises configuring the scanned data such that at least one of a global logon
3 password, an Internet protocol (IP) address, and a media access control (MAC)
4 address of a data receiving device that received the transmitted data is verified.

1 7. The method of claim 1, wherein transmitting the scanned data
2 comprises faxing the scanned data.

1 8. The method of claim 1, wherein transmitting the scanned data
2 comprises digitally sending the scanned data as an email attachment.

1 9. The method of claim 1, wherein determining if the transmitted data
2 may be accessed comprises verifying required recipient-specific security information
3 provided by a recipient that intends to access the transmitted data.

1 10. The method of claim 9, wherein verifying required recipient-specific
2 security information comprises verifying at least one of a recipient password and
3 recipient biometric information.

1 11. The method of claim 1, wherein determining if the transmitted data
2 may be accessed comprises verifying required machine-specific security information.

1 12. The method of claim 11, wherein verifying required machine-specific
2 security information comprises verifying at least one of a global logon password, an
3 Internet protocol (IP) address, and a media access control (MAC) address of a data
4 receiving device that received the transmitted data is verified.

1 13. The method of claim 1, further comprising providing access to the
2 transmitted data if it is determined that the transmitted data may be accessed at the
3 recipient end.

1 14. The method of claim 13, wherein providing access comprises at least
2 one of printing out the transmitted data and opening an email attachment that
3 comprises the transmitted data.

1 15. A system for providing recipient-end security for transmitted data, the
2 system comprising:

3 means for configuring scanned data representative of a hard copy document so
4 as to require recipient-end security at a recipient end of a transmission path;

5 means for determining if the scanned data may be accessed at the recipient end
6 by requiring at least one of recipient-specific security information and machine-
7 specific security information; and

8 means for denying access to the transmitted data if it is determined that the
9 required security information is not correct.

1 16. The system of claim 15, wherein the means for configuring comprise
2 means for configuring the scanned data such that at least one of a recipient password
3 and recipient biometric information is required to access the scanned data.

1 17. The system of claim 15, wherein the means for configuring comprise
2 means for configuring the scanned data such that at least one of a global logon
3 password, an Internet protocol (IP) address, and a media access control (MAC)
4 address of a data receiving device that received the transmitted data is required to
5 access the scanned data.

1 18. The system of claim 15, wherein the means for determining comprise
2 means for verifying at least one of a recipient password and recipient biometric
3 information.

1 19. The system of claim 15, wherein the means for verifying comprise
2 means for verifying at least one of a global logon password, an Internet protocol (IP)
3 address, and a media access control (MAC) address of a data receiving device that
4 received the transmitted data is verified.

1 20. A system stored on a computer-readable medium, the system
2 comprising:
3 sender-end logic adapted to execute on a data transmitting device, the sender-
4 end logic being configured to configure data scanned by the data transmitting device
5 so as to require recipient-end security at a recipient end of a transmission path; and
6 recipient-end logic adapted to execute on a data receiving device, the recipient-
7 end logic being configured to determine if the scanned data may be accessed at the
8 recipient end by verifying at least one of recipient-specific security information
9 provided by a recipient of the scanned data and machine-specific security information
10 of the data receiving device.

1 21. The system of claim 20, wherein the sender-end logic is configured to
2 require at least one of a recipient password and recipient biometric information of the
3 recipient prior to access of the scanned data.

1 22. The system of claim 20, wherein the sender-end logic is configured to
2 require at least one of a global logon password, an Internet protocol (IP) address, and a
3 media access control (MAC) address of a data receiving device that received the
4 transmitted data is verified before a recipient access the scanned data.

1 23. The system of claim 20, wherein the recipient-end logic is configured
2 to verify at least one of a recipient password and recipient biometric information prior
3 to providing access to the scanned data.

1 24. The system of claim 20, wherein the recipient-end logic is configured
2 to verify at least one of a global logon password, an Internet protocol (IP) address, and
3 a media access control (MAC) address of a data receiving device that received the
4 transmitted data prior to providing access to the scanned data.

1 25. A sender-end security manager stored on a computer-readable medium
2 of a data transmitting device, the manager comprising:
3 logic configured to identify a type of recipient-end security to provide for a
4 data scanned by the data transmitting device; and
5 logic configured to configure the scanned data to facilitate the identified type
6 of recipient-end security.

1 26. The manager of claim 25, wherein the logic configured to configure the
2 scanned data comprises logic configured to add security information to the scanned
3 data that is to be used as a reference against recipient-specific security information
4 entered by a recipient of the scanned data.

1 27. The manager of claim 25, wherein the logic configured to configure the
2 scanned data comprises logic configured to add an executable that is configured to
3 verify at least one of recipient-specific security information entered by a recipient of
4 the scanned data and machine-specific security information of a data receiving device
5 that received the scanned data.

1 28. The manager of claim 25, wherein the logic configured to configure the
2 scanned data comprises logic configured to add an instruction to the scanned data that
3 indicates to a recipient-end security manager what tasks are to be performed to
4 provided recipient-end security.

1 29. A recipient-end security manager stored on a computer-readable
2 medium of a data receiving device, the manager comprising:
3 logic configured to identify a type of recipient-end security that is required to
4 access data that has been received by the data receiving device; and
5 logic configured to verify recipient-end security information prior to enabling
6 access to the data.

1 30. The manager of claim 29, wherein the logic configured to verify
2 recipient-end security information comprises logic configured to verify at least one of
3 a recipient password and recipient biometric information.

1 31. The manager of claim 29, wherein the logic configured to verify
2 recipient-end security information comprises logic configured to verify at least one of
3 a global logon password, an Internet protocol (IP) address, and a media access control
4 (MAC) address of the data receiving device.